the cognizant COTP a Facility Vulnerability and Security Measures Summary (Form CG–6025) in appendix A to part 105—Facility Vulnerability and Security (CG–6025).

§ 105.145 Maritime Security (MARSEC) Directive.

Each facility owner or operator subject to this part must comply with any instructions contained in a MARSEC Directive issued under §101.405 of this subchapter.

§ 105.150 Right to appeal.

Any person directly affected by a decision or action taken under this part, by or on behalf of the Coast Guard, may appeal as described in §101.420 of this subchapter.

Subpart B—Facility Security Requirements

§ 105.200 Owner or operator.

(a) Each facility owner or operator must ensure that the facility operates in compliance with the requirements of this part.

(b) For each facility, the facility owner or operator must:

(1) Define the security organizational structure and provide each person exercising security duties and responsibilities within that structure the support needed to fulfill those obligations;

(2) Designate, in writing, by name or by title, a Facility Security Officer (FSO) and identify how the officer can be contacted at any time;

(3) Ensure that a Facility Security Assessment (FSA) is conducted;

(4) Ensure the development and submission for approval of an FSP;

(5) Ensure that the facility operates in compliance with the approved FSP;

(6) Ensure that the TWIC program is properly implemented as set forth in this part, including:

(i) Ensuring that only individuals who hold a TWIC and are authorized to be in the secure area in accordance with the FSP are permitted to escort;

(ii) Identifying what action is to be taken by an escort, or other authorized individual, should individuals under escort engage in activities other than those for which escorted access was granted; and

(iii) Notifying facility employees, and passengers if applicable, of what parts of the facility are secure areas and public access areas, as applicable, and ensuring such areas are clearly marked.

(7) Ensure that restricted areas are controlled and TWIC provisions are coordinated, if applied to such restricted areas;

(8) Ensure that adequate coordination of security issues takes place between the facility and vessels that call on it, including the execution of a Declaration of Security (DoS) as required by this part;

(9) Ensure coordination of shore leave for vessel personnel or crew change-out, as well as access through the facility for visitors to the vessel (including representatives of seafarers' welfare and labor organizations), with vessel operators in advance of a vessel's arrival. In coordinating such leave, facility owners or operators may refer to treaties of friendship, commerce, and navigation between the U.S. and other nations. The text of these treaties can be found at *http://www.marad.dot.gov/Programs/treaties.html;*

(10) Ensure, within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level;

(11) Ensure security for unattended vessels moored at the facility;

(12) Ensure the report of all breaches of security and transportation security incidents to the National Response Center in accordance with part 101 of this chapter;

(13) Ensure consistency between security requirements and safety requirements;

(14) Inform facility personnel of their responsibility to apply for and maintain a TWIC, including the deadlines and methods for such applications, and of their obligation to inform TSA of any event that would render them ineligible for a TWIC, or which would invalidate their existing TWIC;

(15) Ensure that protocols consistent with section 105.255(c) of this part, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or who have applied for and

not yet received a TWIC, are in place; and

(16) If applicable, ensure that protocols consistent with §105.257 of this part, for dealing with newly hired employees who have applied for and not yet received a TWIC, are in place.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003; USCG–2006–24196, 72 FR 3582, Jan. 25, 2007]

§105.205 Facility Security Officer (FSO).

(a) *General.* (1) The FSO may perform other duties within the owner's or operator's organization, provided he or she is able to perform the duties and responsibilities required of the FSO.

(2) The same person may serve as the FSO for more than one facility, provided the facilities are in the same COTP zone and are not more than 50 miles apart. If a person serves as the FSO for more than one facility, the name of each facility for which he or she is the FSO must be listed in the Facility Security Plan (FSP) of each facility for which or she is the FSO.

(3) The FSO may assign security duties to other facility personnel; however, the FSO retains the responsibility for these duties.

(4) The FSO must maintain a TWIC.

(b) *Qualifications.* (1) The FSO must have general knowledge, through training or equivalent job experience, in the following:

(i) Security organization of the facility;

(ii) General vessel and facility operations and conditions;

(iii) Vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels;

(iv) Emergency preparedness, response, and contingency planning;

(v) Security equipment and systems, and their operational limitations; and

(vi) Methods of conducting audits, inspections, control, and monitoring techniques.

(2) In addition to knowledge and training required in paragraph (b)(1) of this section, the FSO must have knowledge of and receive training in the following, as appropriate:

(i) Relevant international laws and codes, and recommendations;

(ii) Relevant government legislation and regulations;

(iii) Responsibilities and functions of local, State, and Federal law enforcement agencies;

(iv) Security assessment methodology;

(v) Methods of facility security surveys and inspections;

(vi) Instruction techniques for security training and education, including security measures and procedures;

(vii) Handling sensitive security information and security related communications;

(viii) Current security threats and patterns;

(ix) Recognizing and detecting dangerous substances and devices;

(x) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;

(xi) Techniques used to circumvent security measures;

(xii) Conducting physical searches and non-intrusive inspections;

(xiii) Conducting security drills and exercises, including exercises with vessels; and

(xiv) Assessing security drills and exercises.

(xv) Knowledge of TWIC requirements.

(c) *Responsibilities.* In addition to those responsibilities and duties specified elsewhere in this part, the FSO must, for each facility for which he or she has been designated:

(1) Ensure that the Facility Security Assessment (FSA) is conducted;

(2) Ensure the development and implementation of a FSP;

(3) Ensure that an annual audit is conducted, and if necessary that the FSA and FSP are updated;

(4) Ensure the FSP is exercised per §105.220 of this part;

(5) Ensure that regular security inspections of the facility are conducted;

(6) Ensure the security awareness and vigilance of the facility personnel;

(7) Ensure adequate training to personnel performing facility security duties;

(8) Ensure that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;

(9) Ensure the maintenance of records required by this part;

(10) Ensure the preparation and the submission of any reports as required by this part;

(11) Ensure the execution of any required Declarations of Security with Masters, Vessel Security Officers or their designated representatives;

(12) Ensure the coordination of security services in accordance with the approved FSP;

(13) Ensure that security equipment is properly operated, tested, calibrated, and maintained;

(14) Ensure the recording and reporting of attainment changes in MARSEC Levels to the owner or operator and the cognizant COTP;

(15) When requested, ensure that the Vessel Security Officers receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility;

(16) Ensure notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident;

(17) Ensure that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP; and

(18) Ensure that all facility personnel are briefed of changes in security conditions at the facility.

(19) Ensure the TWIC program is being properly implemented.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003; USCG–2006–24196, 72 FR 3583, Jan. 25, 2007]

§ 105.210 Facility personnel with security duties.

Facility personnel responsible for security duties must maintain a TWIC, and must have knowledge, through training or equivalent job experience, in the following, as appropriate:

(a) Knowledge of current security threats and patterns;

(b) Recognition and detection of dangerous substances and devices;

(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(d) Techniques used to circumvent security measures;

(e) Crowd management and control techniques;

(f) Security related communications;

(g) Knowledge of emergency procedures and contingency plans;

(h) Operation of security equipment and systems;

(i) Testing, calibration, and maintenance of security equipment and systems;

(j) Inspection, control, and monitoring techniques;

(k) Relevant provisions of the Facility Security Plan (FSP);

(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; and

(m) The meaning and the consequential requirements of the different MARSEC Levels.

(n) Familiar with all relevant aspects of the TWIC program and how to carry them out.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended by USCG–2006–24196, 72 FR 3583, Jan. 25, 2007]

§ 105.215 Security training for all other facility personnel.

All other facility personnel, including contractors, whether part-time, full-time, temporary, or permanent, must have knowledge of, through training or equivalent job experience, in the following, as appropriate:

(a) Relevant provisions of the Facility Security Plan (FSP);

(b) The meaning and the consequential requirements of the different MARSEC Levels as they apply to them, including emergency procedures and contingency plans;

(c) Recognition and detection of dangerous substances and devices;

(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and

(e) Techniques used to circumvent security measures.

(f) Familiar with all relevant aspects of the TWIC program and how to carry them out.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003; USCG–2006–24196, 72 FR 3583, Jan. 25, 2007]

§ 105.220 Drill and exercise requirements.

(a) *General.* (1) Drills and exercises must test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the Facility Security Plan (FSP). They must enable the Facility Security Officer (FSO) to identify any related security deficiencies that need to be addressed.

(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the facility reports attainment to the cognizant COTP.

(b) *Drills.* (1) The FSO must ensure that at least one security drill is conducted every 3 months. Security drills may be held in conjunction with nonsecurity drills, where appropriate.

(2) Drills must test individual elements of the FSP, including response to security threats and incidents. Drills should take into account the types of operations of the facility, facility personnel changes, the type of vessel the facility is serving, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.

(3) If a vessel is moored at the facility on the date the facility has planned to conduct any drills, the facility cannot require the vessel or vessel personnel to be a part of or participate in the facility's scheduled drill.

(c) *Exercises.* (1) Exercises must be conducted at least once each calendar year, with no more than 18 months between exercises.

(2) Exercises may be:

(i) Full scale or live;

(ii) Tabletop simulation or seminar;

(iii) Combined with other appropriate exercises; or

(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.

(3) Exercises may be facility-specific or part of a cooperative exercise program with applicable facility and vessel security plans or comprehensive port exercises.

(4) Each exercise must test communication and notification procedures, and elements of coordination, resource availability, and response.

(5) Exercises are a full test of the security program and must include substantial and active participation of FSOs, and may include government authorities and vessels visiting the facility. Requests for participation of Company and Vessel Security Officers in joint exercises should consider the security and work implications for the vessel.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003]

§ 105.225 Facility recordkeeping requirements.

(a) Unless otherwise specified in this section, the Facility Security Officer (FSO) must keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request.

(b) Records required by this section may be kept in electronic format. If kept in an electronic format, they must be protected against unauthorized deletion, destruction, or amendment. The following records must be kept:

(1) *Training.* For training under § 105.210, the date of each session, duration of session, a description of the training, and a list of attendees;

(2) *Drills and exercises.* For each drill or exercise, the date held, description of drill or exercise, list of participants, and any best practices or lessons learned which may improve the Facility Security Plan (FSP);

(3) *Incidents and breaches of security.* For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response;

(4) *Changes in MARSEC Levels.* For each change in MARSEC Level, the date and time of notification received, and time of compliance with additional requirements;

(5) *Maintenance, calibration, and testing of security equipment.* For each occurrence of maintenance, calibration, and testing, record the date and time,

and the specific security equipment involved;

(6) *Security threats.* For each security threat, the date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;

(7) *Declaration of Security (DoS)* A copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period; and

(8) *Annual audit of the FSP.* For each annual audit, a letter certified by the FSO stating the date the audit was completed.

(c) Any record required by this part must be protected from unauthorized access or disclosure.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003]

§ 105.230 Maritime Security (MARSEC) Level coordination and implementation.

(a) The facility owner or operator must ensure the facility operates in compliance with the security requirements in this part for the MARSEC Level in effect for the port.

(b) When notified of an increase in the MARSEC Level, the facility owner and operator must ensure:

(1) Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the MARSEC Level change are notified of the new MARSEC Level and the Declaration of Security is revised as necessary;

(2) The facility complies with the required additional security measures within 12 hours; and

(3) The facility reports compliance or noncompliance to the COTP.

(c) For MARSEC Levels 2 and 3, the Facility Security Officer must inform all facility personnel about identified threats, and emphasize reporting procedures and stress the need for increased vigilance.

(d) An owner or operator whose facility is not in compliance with the requirements of this section, must inform the COTP and obtain approval prior to interfacing with a vessel or continuing operations.

(e) At MARSEC Level 3, in addition to the requirements in this part, a facility owner or operator may be required to implement additional measures, pursuant to 33 CFR part 6, 160, or 165, as appropriate, which may include but are not limited to:

(1) Use of waterborne security patrol;

(2) Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and

(3) Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.

§ 105.235 Communications.

(a) The Facility Security Officer must have a means to effectively notify facility personnel of changes in security conditions at the facility.

(b) Communication systems and procedures must allow effective and continuous communications between the facility security personnel, vessels interfacing with the facility, the cognizant COTP, and national and local authorities with security responsibilities.

(c) At each active facility access point, provide a means of contacting police, security control, or an emergency operations center, by telephones, cellular phones, and/or portable radios, or other equivalent means.

(d) Facility communications systems must have a backup means for both internal and external communications.

§ 105.240 Procedures for interfacing with vessels.

The facility owner or operator must ensure that there are measures for interfacing with vessels at all MARSEC Levels.

§ 105.245 Declaration of Security (DoS).

(a) Each facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a vessel.

(b) At MARSEC Level 1, a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo,

in bulk, must comply with the following:

(1) Prior to the arrival of a vessel to the facility, the Facility Security Officer (FSO) and Master, Vessel Security Officer (VSO), or their designated representatives must coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility; and

(2) Upon the arrival of the vessel at the facility, the FSO and Master, VSO, or their designated representative, must sign the written DoS.

(c) Neither the facility nor the vessel may embark or disembark passengers, nor transfer cargo or vessel stores until the DoS has been signed and implemented.

(d) At MARSEC Levels 2 and 3, the FSOs, or their designated representatives, of facilities interfacing with manned vessels subject to part 104, of this subchapter must sign and implement DoSs as required in (b)(1) and (2) of this section.

(e) At MARSEC Levels 1 and 2, FSOs of facilities that frequently interface with the same vessel may implement a continuing DoS for multiple visits, provided that:

(1) The DoS is valid for a specific MARSEC Level;

(2) The effective period at MARSEC Level 1 does not exceed 90 days; and

(3) The effective period at MARSEC Level 2 does not exceed 30 days.

(f) When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed in accordance with this section.

(g) A copy of all currently valid continuing DoSs must be kept with the Facility Security Plan.

(h) The COTP may require, at any time, at any MARSEC Level, any facility subject to this part to implement a DoS with the VSO prior to any vessel-to-facility interface when he or she deems it necessary.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003]

§ 105.250 Security systems and equipment maintenance.

(a) Security systems and equipment must be in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.

(b) Security systems must be regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required in § 105.225 of this subpart.

(c) The FSP must include procedures for identifying and responding to security system and equipment failures or malfunctions.

§ 105.255 Security measures for access control.

(a) *General.* The facility owner or operator must ensure the implementation of security measures to:

(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;

(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility;

(3) Control access to the facility; and

(4) Prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.

(b) The facility owner or operator must ensure that the following are specified:

(1) The locations where restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC Level, including those points where TWIC access control provisions will be applied. Each location allowing means of access to the facility must be addressed;

(2) The types of restrictions or prohibitions to be applied and the means of enforcing them;

(3) The means used to establish the identity of individuals not in possession of a TWIC, in accordance with § 101.515 of this subchapter, and procedures for escorting them;

(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level; and

(5) The locations where persons, personal effects and vehicle screenings are to be conducted. The designated screening areas should be covered to

provide for continuous operations regardless of the weather conditions.

(c) The facility owner or operator must ensure that a TWIC program is implemented as follows:

(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with §101.514 of this subchapter. Inspection must include:

(i) A match of the photo on the TWIC to the individual presenting the TWIC;

(ii) Verification that the TWIC has not expired; and

(iii) A visual check of the various security features present on the card to determine whether the TWIC has been tampered with or forged.

(2) If an individual cannot present a TWIC because it has been lost, damaged or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if:

(i) The individual has reported the TWIC as lost, damaged, or stolen to TSA as required in 49 CFR 1572.19(f);

(ii) The individual can present another identification credential that meets the requirements of §101.515 of this subchapter; and

(iii) There are no other suspicious circumstances associated with the individual's claim of loss or theft.

(3) If an individual cannot present his or her TWIC for any other reason than outlined in paragraph (c)(2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside of a secure area.

(4) With the exception of persons granted access according to paragraph (c)(2) of this section, all persons granted unescorted access to secure areas of the facility must be able to produce his or her TWIC upon request.

(5) There must be disciplinary measures in place to prevent fraud and abuse.

(6) The facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of vessels or other transportation conveyances that use the facility.

(d) If the facility owner or operator uses a separate identification system, ensure that it complies and is coordinated with TWIC provisions in this part.

(e) The facility owner or operator must establish in the approved Facility Security Plan (FSP) the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis.

(f) *MARSEC Level 1.* The facility owner or operator must ensure the following security measures are implemented at the facility:

(1) Implement TWIC as set out in paragraph (c) of this section.

(2) Screen persons, baggage (including carry-on items), personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP, excluding government-owned vehicles on official business when government personnel present identification credentials for entry;

(3) Conspicuously post signs that describe security measures currently in effect and clearly state that:

(i) Entering the facility is deemed valid consent to screening or inspection; and

(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter.

(4) Check the identification of any person not holding a TWIC and seeking entry to the facility, including vessel passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check shall include confirming the reason for boarding by examining at least one of the following:

(i) Joining instructions;

(ii) Passenger tickets;

(iii) Boarding passes;

(iv) Work orders, pilot orders, or surveyor orders;

(v) Government identification; or

(vi) Visitor badges issued in accordance with an identification system implemented under paragraph (d) of this section.

(5) Deny or revoke a person's authorization to be on the facility if the person is unable or unwilling, upon the request of facility personnel or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence. Any such incident must be reported in compliance with this part;

(6) Designate restricted areas and provide appropriate access controls for these areas;

(7) Identify access points that must be secured or attended to deter unauthorized access;

(8) Deter unauthorized access to the facility and to designated restricted areas within the facility;

(9) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and

(10) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.

(g) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;

(2) X-ray screening of all unaccompanied baggage;

(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;

(4) Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;

(5) Denying access to visitors who do not have a verified destination;

(6) Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility; or

(7) Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for MARSEC Level 2 in the approved FSP.

(h) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in their approved FSP. These additional security measures may include:

(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;

(2) Performing one or more of the following on unaccompanied baggage:

(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;

(ii) Prepare to restrict or suspend handling of unaccompanied baggage; or

(iii) Refuse to accept unaccompanied baggage.

(3) Being prepared to cooperate with responders and facilities;

(4) Granting access to only those responding to the security incident or threat thereof;

(5) Suspending access to the facility;

(6) Suspending cargo operations;

(7) Evacuating the facility;

(8) Restricting pedestrian or vehicular movement on the grounds of the facility; or

(9) Increasing security patrols within the facility.

[USCG–2006–24196, 72 FR 3583, Jan. 25, 2007]

§ 105.257 Security measures for newly-hired employees.

(a) Newly-hired facility employees may be granted entry to secure areas of the facility for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in paragraph (b) of this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the facility. If TSA does not act upon a TWIC application within 30 days, the cognizant Coast Guard COTP may further extend access to secure areas for

another 30 days. The Coast Guard will determine whether, in particular circumstances, certain practices meet the condition of a new hire being accompanied by another individual with a TWIC. The Coast Guard will issue guidance for use in making these determinations.

(b) Newly-hired facility employees may be granted the access provided for in paragraph (a) of this section if:

(1) The new hire has applied for a TWIC in accordance with 49 CFR part 1572 by completing the full enrollment process, paying the user fee, and is not currently engaged in a waiver or appeal process. The facility owner or operator or the Facility Security Officer (FSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC;

(2) The facility owner or operator or the FSO enters the following information on the new hire into the Coast Guard's Homeport website (*http://homeport.uscg.mil*):

(i) Full legal name, including middle name if one exists;

(ii) Date of birth;

(iii) Social security number (optional);

(iv) Employer name and 24 hour contact information; and

(v) Date of TWIC enrollment.

(3) The new hire presents an identification credential that meets the requirements of §101.515 of this subchapter;

(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the facility owner or operator or FSO have not been informed by the cognizant COTP that the new hire poses a security threat; and

(5) There would be an adverse impact to facility operations if the new hire is not allowed access.

(c) This section does not apply to any individual being hired as a FSO, or any individual being hired to perform facility security duties.

(d) The new hire may not begin working at the facility under the provisions of this section until the owner, operator, or FSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.

[USCG–2006–24196, 72 FR 3584, Jan. 25, 2007]

§105.260 Security measures for restricted areas.

(a) *General.* The facility owner or operator must ensure the designation of restricted areas in order to:

(1) Prevent or deter unauthorized access;

(2) Protect persons authorized to be in the facility;

(3) Protect the facility;

(4) Protect vessels using and serving the facility;

(5) Protect sensitive security areas within the facility;

(6) Protect security and surveillance equipment and systems; and

(7) Protect cargo and vessel stores from tampering.

(b) *Designation of Restricted Areas.* The facility owner or operator must ensure restricted areas are designated within the facility. They must also ensure that all restricted areas are clearly marked and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security. The facility owner or operator may also designate the entire facility as a restricted area. Restricted areas must include, as appropriate:

(1) Shore areas immediately adjacent to each vessel moored at the facility;

(2) Areas containing sensitive security information, including cargo documentation;

(3) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls; and

(4) Areas containing critical facility infrastructure, including:

(i) Water supplies;

(ii) Telecommunications;

(iii) Electrical system; and

(iv) Access points for ventilation and air-conditioning systems;

(5) Manufacturing or processing areas and control rooms;

(6) Locations in the facility where access by vehicles and personnel should be restricted;

(7) Areas designated for loading, unloading or storage of cargo and stores; and

(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.

(c) The owner or operator must ensure that all restricted areas have clearly established security measures to:

(1) Identify which facility personnel are authorized to have access;

(2) Determine which persons other than facility personnel are authorized to have access;

(3) Determine the conditions under which that access may take place;

(4) Define the extent of any restricted area;

(5) Define the times when access restrictions apply;

(6) Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security;

(7) Control the entry, parking, loading and unloading of vehicles;

(8) Control the movement and storage of cargo and vessel stores; and

(9) Control unaccompanied baggage or personal effects.

(d) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include:

(1) Restricting access to only authorized personnel;

(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;

(3) Assigning personnel to control access to restricted areas;

(4) Verifying the identification and authorization of all persons and all vehicles seeking entry;

(5) Patrolling or monitoring the perimeter of restricted areas;

(6) Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized entry or movement within restricted areas;

(7) Directing the parking, loading, and unloading of vehicles within a restricted area;

(8) Controlling unaccompanied baggage and or personal effects after screening;

(9) Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading; and

(10) Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.

(e) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in their approved FSP. These additional security measures may include:

(1) Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas;

(2) Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices;

(3) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;

(4) Restricting parking adjacent to vessels;

(5) Further restricting access to the restricted areas and movements and storage within them;

(6) Using continuously monitored and recorded surveillance equipment;

(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas; or

(8) Establishing and restricting access to areas adjacent to the restricted areas.

(f) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in

their approved FSP. These additional security measures may include:

(1) Restricting access to additional areas;

(2) Prohibiting access to restricted areas, or

(3) Searching restricted areas as part of a security sweep of all or part of the facility.

§ 105.265 Security measures for handling cargo.

(a) *General.* The facility owner or operator must ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to:

(1) Deter tampering;

(2) Prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator;

(3) Identify cargo that is approved for loading onto vessels interfacing with the facility;

(4) Include cargo control procedures at access points to the facility;

(5) Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;

(6) Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;

(7) Ensure the release of cargo only to the carrier specified in the cargo documentation;

(8) When there are regular or repeated cargo operations with the same shipper, coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedure; and

(9) Create, update, and maintain a continuous inventory of all dangerous goods and hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods and hazardous substances.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of measures to:

(1) Unless unsafe to do so, routinely check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling operations for evidence of tampering;

(2) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;

(3) Screen vehicles; and

(4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Conducting check of cargo, containers or other cargo transport units, and cargo storage areas within the facility for evidence of tampering;

(2) Intensifying checks, as appropriate, to ensure that only the documented cargo enters the facility, is temporarily stored there, and then loaded onto the vessel;

(3) Intensifying the screening of vehicles;

(4) Increasing frequency and detail in checking of seals and other methods used to prevent tampering;

(5) Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures;

(6) Increasing the frequency and intensity of visual and physical inspections; or

(7) Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.

(d) *MARSEC Level 3.* In addition to the security measures required for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must ensure the implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels;

(2) Being prepared to cooperate with responders and vessels; or

(3) Verifying the inventory and location of any dangerous goods and hazardous substances, including certain dangerous cargoes, held within the facility and their location.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60541, Oct. 22, 2003]

§ 105.270 Security measures for delivery of vessel stores and bunkers.

(a) *General.* The facility owner or operator must ensure that security measures relating to the delivery of vessel stores and bunkers are implemented to:

(1) Check vessel stores for package integrity;

(2) Prevent vessel stores from being accepted without inspection;

(3) Deter tampering;

(4) For vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation; and

(5) Check vessel stores by the following means:

(i) Visual examination;

(ii) Physical examination;

(iii) Detection devices, such as scanners; or

(iv) Canines.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the implementation of measures to:

(1) Screen vessel stores at the rate specified in the approved Facility Security Plan (FSP);

(2) Require advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;

(3) Screen delivery vehicles at the frequencies specified in the approved FSP; and

(4) Escort delivery vehicles within the facility at the rate specified by the approved FSP.

(c) *MARSEC Level 2.* In addition to the security measures required for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional security measures may include:

(1) Detailed screening of vessel stores;

(2) Detailed screening of all delivery vehicles;

(3) Coordinating with vessel personnel to check the order against the delivery note prior to entry to the facility;

(4) Ensuring delivery vehicles are escorted within the facility; or

(5) Restricting or prohibiting the entry of vessel stores that will not leave the facility within a specified period.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner and operator must ensure implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. Examples of these additional security measures may include:

(1) Checking all vessel stores more extensively;

(2) Restricting or suspending delivery of vessel stores; or

(3) Refusing to accept vessel stores on the facility.

§ 105.275 Security measures for monitoring.

(a) *General.* The facility owner or operator must ensure the implementation of security measures in this section and have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, or surveillance equipment, as specified in the approved Facility Security Plan (FSP), the:

(1) Facility and its approaches, on land and water;

(2) Restricted areas within the facility; and

(3) Vessels at the facility and areas surrounding the vessels.

(b) *MARSEC Level 1.* At MARSEC Level 1, the facility owner or operator must ensure the security measures in this section are implemented at all times, including the period from sunset to sunrise and periods of limited visibility. For each facility, ensure monitoring capability that:

(1) When automatic intrusion-detection devices are used, activates an audible or visual alarm, or both, at a location that is continuously attended or monitored;

(2) Is able to function continually, including consideration of the possible effects of weather or of a power disruption;

(3) Monitors the facility area, including shore and waterside access to it;

(4) Monitors access points, barriers and restricted areas;

(5) Monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and

(6) Limits lighting effects, such as glare, and their impact on safety, navigation, and other security activities.

(c) *MARSEC Level 2.* In addition to the security measures for MARSEC Level 1 in this section, at MARSEC Level 2, the facility owner or operator must also ensure the implementation of additional security measures, as specified for MARSEC Level 2 in the approved FSP. These additional measures may include:

(1) Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage;

(2) Increasing the frequency of foot, vehicle or waterborne patrols;

(3) Assigning additional security personnel to monitor and patrol; or

(4) Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage.

(d) *MARSEC Level 3.* In addition to the security measures for MARSEC Level 1 and MARSEC Level 2, at MARSEC Level 3, the facility owner or operator must also ensure implementation of additional security measures, as specified for MARSEC Level 3 in the approved FSP. These additional security measures may include:

(1) Switching on all lighting within, or illuminating the vicinity of, the facility;

(2) Switching on all surveillance equipment capable of recording activities within or adjacent to the facility;

(3) Maximizing the length of time such surveillance equipment can continue to record; or

(4) Complying with the instructions issued by those responding to the security incident.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

§ 105.280 Security incident procedures.

For each MARSEC Level, the facility owner or operator must ensure the Facility Security Officer and facility security personnel are able to:

(a) Respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations;

(b) Evacuate the facility in case of security threats or breaches of security;

(c) Report security incidents as required in § 101.305 of this subchapter;

(d) Brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and

(e) Secure non-critical operations in order to focus response on critical operations.

§ 105.285 Additional requirements-passenger and ferry facilities.

(a) At all MARSEC Levels, the owner or operator of a passenger or ferry facility must ensure, in coordination with a vessel moored at the facility, that the following security measures are implemented in addition to the requirements of this part:

(1) Establish separate areas to segregate unchecked persons and personal effects from checked persons and personal effects;

(2) Ensure that a defined percentage of vehicles to be loaded aboard are screened prior to loading, in accordance with a MARSEC Directive or other orders issued by the Coast Guard;

(3) Ensure that all unaccompanied vehicles to be loaded on passenger vessels are screened prior to loading;

(4) Deny passenger access to secure and restricted areas unless escorted by authorized facility security personnel; and

(5) In a facility with a public access area designated under § 105.106, provide sufficient security personnel to monitor all persons within the area.

(b) At MARSEC Level 2, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring of the public access area.

(c) At MARSEC Level 3, in addition to the requirements in paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under § 105.106 must increase the intensity of monitoring and assign additional security personnel to monitor the public access area.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003; USCG–2006–24196, 72 FR 3584, Jan. 25, 2007]

§ 105.290 Additional requirements—cruise ship terminals.

At all MARSEC Levels, in coordination with a vessel moored at the facility, the facility owner or operator must ensure the following security measures:

(a) Screen all persons, baggage, and personal effects for dangerous substances and devices;

(b) Check the identification of all persons seeking to enter the facility. Persons holding a TWIC shall be checked as set forth in this part. For persons not holding a TWIC, this check includes confirming the reason for boarding by examining passenger tickets, boarding passes, government identification or visitor badges, or work orders;

(c) Designate holding, waiting, or embarkation areas within the facility's secure area to segregate screened persons and their personal effects awaiting embarkation from unscreened persons and their personal effects;

(d) Provide additional security personnel to designated holding, waiting, or embarkation areas within the facility's secure area; and

(e) Deny individuals not holding a TWIC access to secure and restricted areas unless escorted.

[USCG–2006–24196, 72 FR 3585, Jan. 25, 2007]

§ 105.295 Additional requirements-Certain Dangerous Cargo (CDC) facilities.

(a) At all MARSEC Levels, owners or operators of CDC facilities must ensure the implementation of the following security measures in addition to the requirements of this part:

(1) Escort all visitors, contractors, vendors, and other non-facility employees at all times while on the facility, if access identification is not provided. Escort provisions do not apply to prearranged cargo deliveries;

(2) Control the parking, loading, and unloading of vehicles within a facility;

(3) Require security personnel to record or report their presence at key points during their patrols;

(4) Search unmanned or unmonitored waterfront areas for dangerous substances and devices prior to a vessel's arrival at the facility; and

(5) Provide an alternate or independent power source for security and communications systems.

(b) At MARSEC Level 2, in addition to the requirements for MARSEC Level 1, owners or operators of CDC facilities must ensure the implementation of the following security measures:

(1) Release cargo only in the presence of the Facility Security Officer (FSO) or a designated representative of the FSO; and

(2) Continuously patrol restricted areas.

(c) At MARSEC Level 3, in addition to the requirements for MARSEC Level 1 and MARSEC Level 2, owners or operators of CDC facilities must ensure the facilities are continuously guarded and restricted areas are patrolled.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

§ 105.296 Additional requirements-barge fleeting facilities.

(a) At MARSEC Level 1, in addition to the requirements of this part, an owner or operator of a barge fleeting facility must ensure the implementation of the following security measures:

(1) Designate one or more restricted areas within the barge fleeting facility to handle those barges carrying, in bulk, cargoes regulated by 46 CFR

chapter I, subchapters D or O, or Certain Dangerous Cargoes;

(2) Maintain a current list of vessels and cargoes in the designated restricted area; and

(3) Ensure that at least one towing vessel is available to service the fleeting facility for every 100 barges within the facility.

(4) Control access to the barges once tied to the fleeting area by implementing TWIC as described in §105.255 of this part.

(b) At MARSEC Level 2, in addition to the requirements of this part and MARSEC Level 1 requirements, an owner or operator of a barge fleeting facility must ensure security personnel are assigned to monitor or patrol the designated restricted area within the barge fleeting facility.

(c) At MARSEC Level 3, in addition to the requirements of this part and MARSEC Level 2 requirements, an owner or operator of a barge fleeting facility must ensure that both land and waterside perimeters of the designated restricted area within the barge fleeting facility are continuously monitored or patrolled.

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003; USCG–2006–24196, 72 FR 3585, Jan. 25, 2007]

Subpart C—Facility Security Assessment (FSA)

§105.300 General.

(a) The Facility Security Assessment (FSA) is a written document that is based on the collection of background information, the completion of an on-scene survey and an analysis of that information.

(b) A common FSA may be conducted for more than one similar facility provided the FSA reflects any facility-specific characteristics that are unique.

(c) Third parties may be used in any aspect of the FSA if they have the appropriate skills and if the Facility Security Officer (FSO) reviews and accepts their work.

(d) Those involved in a FSA must be able to draw upon expert assistance in the following areas, as appropriate:

(1) Knowledge of current security threats and patterns;

(2) Recognition and detection of dangerous substances and devices;

(3) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;

(4) Techniques used to circumvent security measures;

(5) Methods used to cause a security incident;

(6) Effects of dangerous substances and devices on structures and facility services;

(7) Facility security requirements;

(8) Facility and vessel interface business practices;

(9) Contingency planning, emergency preparedness, and response;

(10) Physical security requirements;

(11) Radio and telecommunications systems, including computer systems and networks;

(12) Marine or civil engineering; and

(13) Facility and vessel operations.

§105.305 Facility Security Assessment (FSA) requirements.

(a) *Background.* The facility owner or operator must ensure that the following background information, if applicable, is provided to the person or persons who will conduct the assessment:

(1) The general layout of the facility, including:

(i) The location of each active and inactive access point to the facility;

(ii) The number, reliability, and security duties of facility personnel;

(iii) Security doors, barriers, and lighting;

(iv) The location of restricted areas;

(v) The emergency and stand-by equipment available to maintain essential services;

(vi) The maintenance equipment, cargo spaces, storage areas, and unaccompanied baggage storage;

(vii) Location of escape and evacuation routes and assembly stations; and

(viii) Existing security and safety equipment for protection of personnel and visitors;

(2) Response procedures for fire or other emergency conditions;

(3) Procedures for monitoring facility and vessel personnel, vendors, repair technicians, and dock workers;